Jméno: _____ Datum: _____ Body: _____

VPN pro vzdálený přístup

Zabezpečení koncových bodů vzdálené pracovní síly, vícefaktorová autentizace a konfigurace tunelů IPsec.

VPN PRO VZDÁLENÝ PŘÍSTUP – PŘEHLED UČIVA

STUDENT
STUDENTSKÝ STATUS
Dráha obránce sítě

ZABEZPEČENÝ
STAV PŘIPOJENÍ
Stínění datových paketů

AKTIVNÍ
OCHRANA PROTI ÚNIKŮM
Ochrana proti únikům DNS a IPv6

Vítejte! Tento balíček aktivit vás provede sítěmi VPN pro vzdálený přístup. Prozkoumáte tunely client-to-site, vícefaktorová přihlášení, kontroly stavu koncových bodů, limity šířky pásma a bezpečnostní auditování syslogu.

KONTROLNÍ BODY PRACOVNÍHO LISTU

- [ ] **Část 1-4: Zvládněte konfigurace VPN a zabezpečení sítě.**
- [ ] **Část 5-7: Vyřešte křížovku a osmisměrku.**
- [ ] **Část 8-9: Vyřešte případové studie a šifrovací výzvu.**
- [ ] **Část 10: Projděte si stránky se základními i pokročilými FAQ.**
- [ ] **Část 11: Prozkoumejte 10 zajímavých faktů z praxe.**
- [ ] **Bonus: výzva Mysli rychle.**

Otevřete průvodce nejlepšími VPN od VPN.com

URL: https://www.vpn.com/cs/vpn/nejlepsi-vpn-pro-firmy/vzdaleny-pristup/

Váš studijní plán: VPN pro vzdálený přístup

- Zabezpečit koncové body vzdálené pracovní síly přistupující k uzlům lokální sítě.
- Nakonfigurujte politiky vícefaktorové autentizace pro vzdálená přihlášení.
- Nastavte konfigurace client-to-site IPsec a OpenVPN.
- Proveďte audit logů vzdálených připojení kvůli porušením řízení přístupu.
- Zavést kontroly stavu zařízení před udělením síťového přístupu.
- Optimalizujte propustnost serveru, aby nedošlo k zahlcení šířky pásma při práci na dálku.

VPN PRO VZDÁLENÝ PŘÍSTUP – POKYNY

Odpovězte na otázky s výběrem odpovědí a otázky pravda/nepravda, doplňte věty s vynechanými slovy pomocí banky slov, přiřaďte definice a vyřešte křížovku a osmisměrku. Uplatněte své znalosti na kontroly stavu zařízení a vícefaktorová přihlášení. Zakončete bonusovou aktivitou Mysli rychle.

TUNELY CLIENT-TO-SITE A SHODA KONCOVÝCH BODŮ (ÚVOD)

VPN pro vzdálený přístup vytvářejí zabezpečené tunely client-to-site pro zaměstnance mimo pracoviště. Zabezpečení těchto připojení vyžaduje vynucování přihlášení s vícefaktorovým ověřováním (MFA), kontroly stavu a souladu koncových zařízení a audit logů přes centrální syslog kolektory.

PŘEČTĚTE SI POZORNĚ KAŽDÝ KONTROLNÍ BOD A VYBERTE NEBO NAPIŠTE SPRÁVNOU ODPOVĚĎ.

Kontrolní bod 1: Výzva s výběrem odpovědí

1. **1. Jaký autentizační standard by měly portály VPN pro vzdálený přístup vyžadovat?**
   - A) Vícefaktorové
   - B) Jeden faktor
   - C) Nešifrováno
   - D) Místní host

2. **2. Jaký protokol je standardem pro zabezpečení client-to-site připojení při práci na dálku?**
   - A) OpenVPN
   - B) SOCKS5
   - C) PPTP
   - D) FTP

3. **3. Jaká kontrola ověřuje před připojením, zda je vzdálený notebook čistý?**
   - A) Kontrola stavu zařízení
   - B) Test rychlosti
   - C) Test pingu
   - D) Množství paměti

4. **4. Kde se ukládají logy připojení vzdálených pracovníků pro bezpečnostní audit?**
   - A) Syslog server
   - B) Klíč registru
   - C) Paměť klienta
   - D) Webový prohlížeč

5. **5. K jakému problému dochází, když počet vzdálených pracovníků překročí kapacitu šířky pásma brány?**
   - A) Škrcení šířky pásma
   - B) Únik DNS
   - C) Průchod handshake
   - D) Odhalení IP

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. Vícefaktorové ověřování přidává druhotný ověřovací token pro zabezpečení vzdálených přihlášení.

○ Pravda ○ Nepravda

7 Otázka 7

7. Kontroly stavu zařízení povolují vzdáleným zařízením s vypnutými firewally přístup k privátním serverům.

○ Pravda ○ Nepravda

8 Otázka 8

8. Logy VPN pro vzdálený přístup jsou zásadní pro dohledání neoprávněného vstupu do firemní sítě.

○ Pravda ○ Nepravda

9 Otázka 9

9. OpenVPN a IPsec jsou zastaralé protokoly, které nedokážou šifrovat data vzdálených klientů.

○ Pravda ○ Nepravda

10 Otázka 10

10. K zahlcení šířky pásma brány dochází, když vzdálený provoz překročí kapacitu síťové karty.

○ Pravda ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

Přečtěte si každou větu níže a doplňte do vynechaného místa správný termín ze slovní banky.

1. Vzdálená přihlášení k firemním portálům musí kvůli ochraně vyžadovat ověřování, které je _____ .

2. Vzdálení klienti šifrují data v tunelu standardními protokoly, jako je _____ .

3. Zařízení musí před vpuštěním do sítě projít kontrolou, která ověřuje jeho _____ .

4. Auditovatelné záznamy o přístupech se průběžně odesílají na centrální server _____ .

5. Při silném provozu během pracovní doby se může vyčerpat _____ brány.

6. Klient-serverové _____ obsluhují ve Windows a macOS ovladače virtuálních adaptérů.

ZÁSOBNÍK SLOV

FIREWALL OPENVPN STAV ZABEZPEČENÍ SYSLOG ŠIFROVÁNÍ ŠÍŘKA PÁSMA TUNELOVÁNÍ VÍCEFAKTOROVÉ

Sem napište své odpovědi:

1.
2.
3.
4.
5.
6.

Kontrolní bod 4: Přiřazování klíčových pojmů

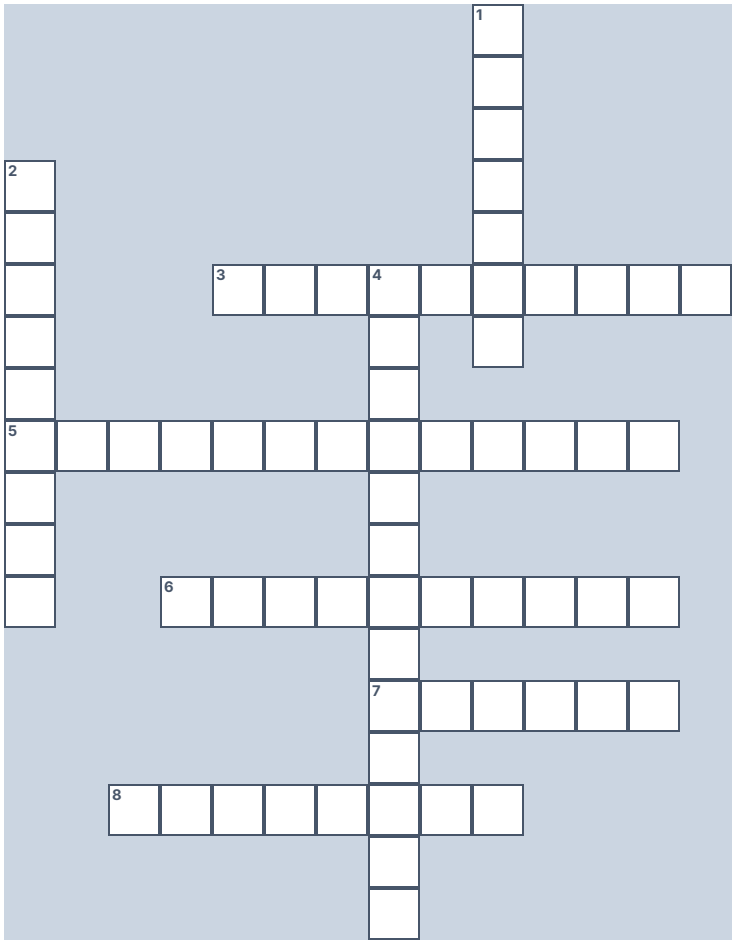
PŘIŘAZOVÁNÍ DEFINIC

Přiřaďte každý slovníčkový pojem vlevo k jeho správné definici vpravo zapsáním odpovídajícího písmene (A–H) do vyplnitelného pole.

☐	1. VÍCEFAKTOROVÉ	A	Zapouzdřování dat v zabezpečené cestě.
☐	2. OPENVPN	B	Centrální kolektor bezpečnostních logů.
☐	3. STAV ZABEZPEČENÍ	C	Limit datové kapacity sítě.
☐	4. SYSLOG	D	Standardní protokol client-to-site.
☐	5. ŠÍŘKA PÁSMA	E	Ověřování stavu vzdáleného zařízení.
☐	6. ŠIFROVÁNÍ	F	Pravidla systému filtrování provozu.
☐	7. TUNELOVÁNÍ	G	Kryptografické zamíchání paketů.
☐	8. FIREWALL	H	Zabezpečení přihlášení vyžadující dodatečné tokeny.

Kontrolní bod 5: Křížovka

Vyřešte křížovku zapisováním písmen do aktivních bílých políček. Čísla odpovídají nápovědám níže.



VODOROVNÉ NÁPOVĚDY

3. Limit datové kapacity sítě (10)

5. Zabezpečení přihlášení vyžadující další tokeny (13)

6. Zapouzdření dat do zabezpečené cesty (10)

7. Centrální kolektor bezpečnostních logů (6)

8. Pravidla systému filtrování provozu (8)

SVISLÉ NÁPOVĚDY

1. Standardní protokol client-to-site (7)

2. Kryptografické zakódování paketů (9)

4. Ověřování zdravotního stavu vzdáleného zařízení (13)

Kontrolní bod 5, alternativa: Přístupná zadání křížovky

Uživatelé čteček obrazovky a klávesnice mohou odpovědi křížovky zapisovat přímo do textových polí níže.

VODOROVNÉ NÁPOVĚDY

3 vodorovně: Limit datové kapacity sítě (10 písmen):

5 vodorovně: Zabezpečení přihlášení vyžadující další tokeny (13 písmen):

6 vodorovně: Zapouzdření dat do zabezpečené cesty (10 písmen):

7 vodorovně: Centrální kolektor bezpečnostních logů (6 písmen):

8 vodorovně: Pravidla systému filtrování provozu (8 písmen):

SVISLÉ NÁPOVĚDY

1 svisle: Standardní protokol client-to-site (7 písmen):

2 svisle: Kryptografické zakódování paketů (9 písmen):

4 svisle: Ověřování zdravotního stavu vzdáleného zařízení (13 písmen):

Kontrolní bod 6: Hledání skrytých slov

Najděte 8 klíčových pojmů skrytých v mřížce níže. Slova mohou být vodorovně, svisle nebo úhlopříčně.

U X T G A Ť Y A Q Ú O O Z P H
V R Ť H Q M Ů U P Ú U K A E F
A P Ň L Á O S Ů Ě F R Ř X I Ý
T J J Ů J Z W Á Y G Q J R I Ž
S I Í Ň A E H Á P T O E A J É
A W E K Ž K Ď L Ř A W L Ň J A
L Ě P K O Č Ň C D A K G S I B
O Á P S M Q V U L I Ý Ř Ě Y Z
R Š F Y W H É L S U Ó Ú Í K S
T S D Í N Á V O R F I Š Ť Š T
N V Í C E F A K T O R O V É M
O Q L O P E N V P N Ň T H K Q
K H T U N E L O V Á N Í Z P M
W Ú O Ý Ř Ř Á Á M Q Ň Á L I É
Í O Ý B Ž Ž Z B Ň Ů Y N Č É P

SEZNAM SLOV

VÍCEFAKTOROVÉ OPENVPN KONTROLASTAVU SYSLOG ŠÍŘKAPÁSMA
ŠIFROVÁNÍ TUNELOVÁNÍ FIREWALL

Kontrolní bod 6, alternativa: Přístupné přiřazování slovíček

Přiřaďte každý z 8 slovníčkových pojmů z osmisměrky k jeho správné definici zapsáním písmene (A–H) do prázdného pole.

POJMY SLOVNÍ ZÁSOBY

- **A. VÍCEFAKTOROVÉ**
- **B. OPENVPN**
- **C. KONTROLASTAVU**
- **D. SYSLOG**
- **E. ŠÍŘKAPÁSMA**
- **F. ŠIFROVÁNÍ**
- **G. TUNELOVÁNÍ**
- **H. FIREWALL**

DEFINICE A POLE K PŘIŘAZENÍ

1. Centrální kolektor bezpečnostních logů.
2. Pravidla systému filtrování provozu.
3. Zapouzdření dat do zabezpečené cesty.
4. Kryptografické zakódování paketů.
5. Standardní protokol client-to-site.
6. Limit datové kapacity sítě.
7. Ověřování zdravotního stavu vzdáleného zařízení.
8. Zabezpečení přihlášení vyžadující další tokeny.

Kontrolní bod 7: Výzva s přeházenými slovy

Přeuspořádejte písmena níže a odhalte klíčové pojmy a termíny z tohoto pracovního listu. Odpovědi pište do připravených polí.

1. KCOVAÍTRVO ÉFE
2. VROONKALUS TAT
3. ŠPMÁÍAAKSŘ
4. ONLÍEÁVTUN
5. VNNEOPP
6. OLSSGY
7. VŠNÍÁRIOF
8. EIWLFLAR

Bonusová aktivita: Mysli rychle

3 ODPOVĚDI V KAŽDÉ KATEGORII. VYHRÁVÁ, KDO PRVNÍ VYPLNÍ CELÝ SEZNAM.

1	Mýty o VPN			
2	Slova, která popisují Zero Trust			
3	Kancelářské programy, které znáte			
4	Pravidla bezpečné práce na dálku			
5	Věci, které vidí váš poskytovatel internetu			
6	VPN služby, které znáte			
7	Místa, odkud zaměstnanci pracují			
8	Nástroje, které firma používá každý den			
9	Role v IT oddělení			
10	Zařízení, která zaměstnanec může mít			
11	Data, která musí firma chránit			
12	Co udělat po bezpečnostním incidentu			
13	Věci, které mohou narušit videoschůzku			
14	Způsoby bezpečného přihlašování			
15	Důvody, proč dát zaměstnancům VPN			

Kontrolní bod 8: Případové studie VPN a sítí

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

PŘÍPADOVÁ STUDIE 1: VYNUCENÍ MFA



Scénář: Byznys analytik se při práci na dálku pokouší přihlásit do své firemní databáze. Zadá správné uživatelské jméno i heslo, ale portál VPN přístup zablokuje a požaduje kód z fyzického tokenu.

Otázka k diskusi: Která bezpečnostní politika vynucuje tento krok dvojitého ověření?

PŘÍPADOVÁ STUDIE 2: SOULAD S POŽADAVKY NA STAV ZAŘÍZENÍ



Scénář: Externí dodavatel připojuje svůj osobní notebook ke vzdálené firemní síti. Klient VPN spojení okamžitě přeruší a upozorní uživatele, že jeho antivirové definice jsou zastaralé.

Otázka k diskusi: Jaká specializovaná kontrola na bráně VPN zablokovala tento pokus o připojení?

Kontrolní bod 9: Dešifrování šifry

Síťový inženýr zabezpečuje směrovací kanály a klientské tunely. Pomocí níže uvedeného klíče písmeno–číslo dešifrujte zprávu zapsáním odpovídajících písmen do prázdných polí.

ŠIFROVACÍ KLÍČ PÍSMENO–ČÍSLO

A=1 Á=2 B=3 C=4 Č=5 D=6 Ď=7 E=8 É=9 Ě=10 F=11 G=12 H=13 I=14
Í=15 J=16 K=17 L=18 M=19 N=20 Ň=21 O=22 Ó=23 P=24 Q=25 R=26 Ř=27 S=28
Š=29 T=30 Ť=31 U=32 Ú=33 Ů=34 V=35 W=36 X=37 Y=38 Ý=39 Z=40 Ž=41

35 40 6 2 18 8 20 39 24 27 15 28 30 32 24 35 24 20

4 13 26 2 20 15 11 14 26 8 19 20 15

40 1 27 15 40 8 20 15

Dešifrovaná zpráva:

TIP: KAŽDÉ ČÍSLO PŘEDSTAVUJE POZICI DANÉHO PÍSMENE V ABECEDĚ (NAPŘ. 1 = A, 2 = B, 41 = Ž).

Kontrolní bod 10: Základní časté otázky k VPN (část A)

Projděte si nejčastější otázky a odpovědi o virtuálních privátních sítích (VPN) a tunelování.

Q1: Co je VPN se vzdáleným přístupem?

Zabezpečená metoda připojení umožňující zaměstnancům pracujícím mimo pracoviště připojit se přímo k privátním firemním serverům.

Q2: Čím se liší client-to-site od site-to-site?

Client-to-site připojuje jednotlivá uživatelská zařízení, zatímco site-to-site propojuje celé fyzické pobočky.

Q3: Co je kontrola stavu zařízení?

Kontrola, která ověřuje stav zabezpečení vzdáleného zařízení (antivirus, úroveň záplat OS) před udělením přístupu.

Q4: Proč se OpenVPN používá pro vzdálený přístup?

Kvůli jeho silnému bezpečnostnímu protokolu, kompatibilitě napříč platformami a schopnosti zvládat jednotlivá připojení.

Q5: Jak MFA chrání vzdálený přístup?

Přidává sekundární ověřovací token, který zabrání přístupu, i když hesla zaměstnanců uniknou nebo jsou ukradena.

Kontrolní bod 10: Základní časté otázky k VPN (část B)

Projděte si nejčastější otázky a odpovědi o virtuálních privátních sítích (VPN) a tunelování.

Q6: Co je syslog server?

Centralizované úložiště logů, které ukládá události připojení, přihlášení a systémová upozornění pro auditní kontroly souladu.

Q7: Co způsobuje škrcení šířky pásma?

Když souhrnné nároky vzdálených zaměstnanců na šířku pásma překročí rychlostní limit firemní internetové brány.

Q8: Mohu domácí počítač připojit k pracovní VPN?

Pouze pokud zařízení projde firemními audity kontroly stavu a je autorizováno správci IT.

Q9: Co je síťová enkapsulace?

Balení datových paketů při přenosu do šifrovaných hlaviček protokolu k zabezpečení přenosu.

Q10: Jak rozdělené tunelování optimalizuje vzdálený přístup?

Umožňuje zaměstnancům používat místního ISP pro běžné prohlížení a pracovní soubory směrovat přes VPN.

Kontrolní bod 10: Pokročilé časté otázky k VPN (část C)

Prozkoumejte pokročilé technické aspekty VPN tunelovacích protokolů, integrací mobilních klientů a podnikového nasazení.

Q1: Jak ověřování založené na certifikátech posiluje vzdálený přístup?

Váže oprávnění k připojení na předinstalované místní digitální certifikáty a blokuje nespravovaná nebo neautorizovaná zařízení.

Q2: Jaké je bezpečnostní riziko rozděleného tunelování pro práci na dálku?

Vytváří potenciální most, kudy může kompromitované místní zařízení směrovat externí hrozby do privátní sítě.

Q3: Jak kontroly stavu zařízení prověřují nastavení registru?

VPN klient spouští lokální skripty, které se dotazují cest v registru a ověřují, zda aktivně běží podnikový bezpečnostní software.

Q4: Proč syslogy standardně používají UDP port 514?

K rychlému přenosu logů s minimální režií, ačkoli bezpečné konfigurace dnes vyžadují zapouzdření TLS přes TCP.

Q5: Jak firmy řeší úzká hrdla šířky pásma na bráně?

Implementací load balancerů a rozložením vzdáleného provozu mezi regionální serverové uzly.

Kontrolní bod 10: Pokročilé časté otázky k VPN (část D)

Prozkoumejte pokročilé technické aspekty VPN tunelovacích protokolů, integrací mobilních klientů a podnikového nasazení.

Q6: Jaká je funkce virtuálních adaptérů TAP/TUN na vzdálených klientech?

Fungují jako virtuální síťové karty a směrují TCP/IP provoz zařízení přímo do šifrovaného VPN tunelu.

Q7: Jak IKEv2 MOBIKE podporuje mobilitu vzdálených pracovníků?

Dynamicky aktualizuje vazby IP adres a udržuje VPN aktivní, když se uživatel pohybuje mezi Wi-Fi a mobilními daty.

Q8: Jaký je rozdíl mezi děleným a plným tunelováním?

Plné směrování vynucuje průchod veškerého internetového provozu zařízení přes VPN, zatímco rozdělené směrování posílá pouze provoz na firemní cílové IP adresy.

Q9: Jak NAT zařízení zpracovávají vzdálená VPN připojení?

Mapováním rozsahů místních portů na veřejné IP adresy brány pro směrování vracejících se šifrovaných datových paketů.

Q10: Jaké compliance standardy nařizují auditování vzdáleného přístupu?

Standardy jako HIPAA, SOC 2 a PCI DSS vyžadují protokolování a monitorování všech relací vzdáleného připojení.

Část 11: 10 faktů a poznatků o VPN z praxe

Projděte si fakta z praxe o rychlostech VPN šifrování, auditech protokolů, mobilní konektivitě a podnikové práci na dálku.

1. VPN POSTŘEH

VPN pro vzdálený přístup vytvářejí zabezpečené tunely client-to-site pro pracovníky mimo pracoviště.

2. VPN POSTŘEH

Vícefaktorové ověřování vyžadují pravidla compliance k ochraně vzdálených firemních portálů.

3. VPN POSTŘEH

Kontroly stavu zařízení ověřují místní bezpečnostní nastavení klienta před udělením přístupu do privátní sítě.

4. VPN POSTŘEH

Syslog servery agregují protokoly připojení k auditu a detekci pokusů o neoprávněný přístup.

5. VPN POSTŘEH

K zahlcení šířky pásma brány dochází, když souhrnné nároky vzdáleného provozu překročí internetové limity serveru.

6. VPN POSTŘEH

Virtuální síťové adaptéry zapouzdřují síťové dotazy operačního systému do zabezpečených protokolů.

7. POSTŘEH K VPN

Podpora MOBIKE umožňuje vzdáleným klientům přepínat sítě bez výpadku VPN tunelu.

8. POSTŘEH K VPN

Směrování celého provozu tunelem zabezpečuje veškerý internetový provoz pracovníků, ale zvyšuje zátěž firemní brány.

9. POSTŘEH K VPN

Certifikátová autentizace váže autorizaci VPN připojení přímo na hardware spravovaný firmou.

10. VPN POSTŘEH

Rámce jako SOC 2 a PCI DSS očekávají logování a monitorování relací vzdáleného přístupu.

Technické reference a zdroje

Studijní příručka a interaktivní hádanky jsou sestaveny z globálních technických standardů, specifikací a regulačních rámců.

AKADEMICKÉ A OBOROVÉ REFERENCE

[1] VPN.com. (2026). Best VPN for Business: Tested & Ranked By Our Experts.

https://www.vpn.com/vpn/best-vpn-for-business/

[2] NIST. (2020). SP 800-207: Zero Trust Architecture.

https://csrc.nist.gov/pubs/sp/800/207/final

[3] NIST. (2016). SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.

https://csrc.nist.gov/pubs/sp/800/46/r2/final

[4] NordLayer. (n.d.). Secure your network & stay compliant with one toggle-ready platform.

https://nordlayer.com/

[5] IETF. (2006). RFC 4555: IKEv2 Mobility and Multihoming Protocol (MOBIKE).

https://www.rfc-editor.org/rfc/rfc4555

Klíč odpovědí: Kontrolní bod 1 - Výběr z možností

1 **Přihlašovací tokeny** ZABEZPEČENÍ MFA — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Vícefaktorové ověřování vynucuje druhotné ověření přihlášení.

2 **Tunel OpenVPN** CLIENT-TO-SITE — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

OpenVPN je standardní protokol pro zabezpečení tunelů klient-síť.

3 **Audity stavu zařízení** KONTROLA ZAŘÍZENÍ — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Kontroly stavu zařízení skenují koncové body na aktivní firewally a antivirové nástroje.

4 **Agregátor logů** SYSLOG SERVER — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Syslog servery shromažďují protokoly bezpečnostních událostí k monitorování porušení přístupu.

5 **Přetečení karty** ZAHLCENÍ BRÁNY — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

K zahlcení šířky pásma brány dochází, když uživatelský provoz překročí limity serveru.

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

6 **Přihlašovací tokeny** KONTROLY MFA

Správná odpověď: Pravda

POZNÁMKA PRO VYUČUJÍCÍ

Vícefaktorové ověřování vynucuje druhotné ověření přihlášení.

7 **Otázka 7**

Správná odpověď: Nepravda

POZNÁMKA PRO VYUČUJÍCÍ

Kontroly stavu zařízení blokují zařízení s vypnutým firewallem nebo antivirem, takže taková zařízení jsou odmítnuta.

8 **Agregátor logů** SYSLOG SERVER

Správná odpověď: Pravda

POZNÁMKA PRO VYUČUJÍCÍ

Syslog servery shromažďují protokoly bezpečnostních událostí k monitorování porušení přístupu.

9 **Otázka 9**

Správná odpověď: Nepravda

POZNÁMKA PRO VYUČUJÍCÍ

OpenVPN a IPsec jsou aktuální protokoly, které provoz vzdálených klientů šifrují.

10 **Přetečení karty** ZAHLCENÍ BRÁNY

Správná odpověď: Pravda

POZNÁMKA PRO VYUČUJÍCÍ

K zahlcení šířky pásma brány dochází, když uživatelský provoz překročí limity serveru.

Klíče slovní zásoby a hodnoticí rubrika

Hodnoticí rubrika pro vyučující: Udělte 1 bod za každé správné přiřazení (celkem 8 bodů) a kontextový termín (celkem 6 bodů).

KONTROLNÍ BOD 4: KLÍČ K PŘIŘAZOVÁNÍ POJMŮ

H 1. VÍCEFAKTOROVÉ	D 2. OPENVPN	E 3. STAV ZABEZPEČENÍ	B 4. SYSLOG
C 5. ŠÍŘKA PÁSMA	G 6. ŠIFROVÁNÍ	A 7. TUNELOVÁNÍ	F 8. FIREWALL

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 VÍCEFAKTOROVÉ	2 OPENVPN	3 STAV ZABEZPEČENÍ	4 SYSLOG
5 ŠÍŘKA PÁSMA	6 TUNELOVÁNÍ		

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 D – SYSLOG	2 H – FIREWALL	3 G – TUNELOVÁNÍ	4 F – ŠIFROVÁNÍ
5 B – OPENVPN	6 E – ŠÍŘKAPÁSMA	7 C – KONTROLASTAVU	8 A – VÍCEFAKTOROVÉ

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy VÍCEFAKTOROVÉ, OPENVPN a STAV ZABEZPEČENÍ a ke každému uvést příklad.

Případové studie:
Požádejte studenty, aby svá doporučení zdůvodnili fakty z pracovního listu, nikoli domněnkami.

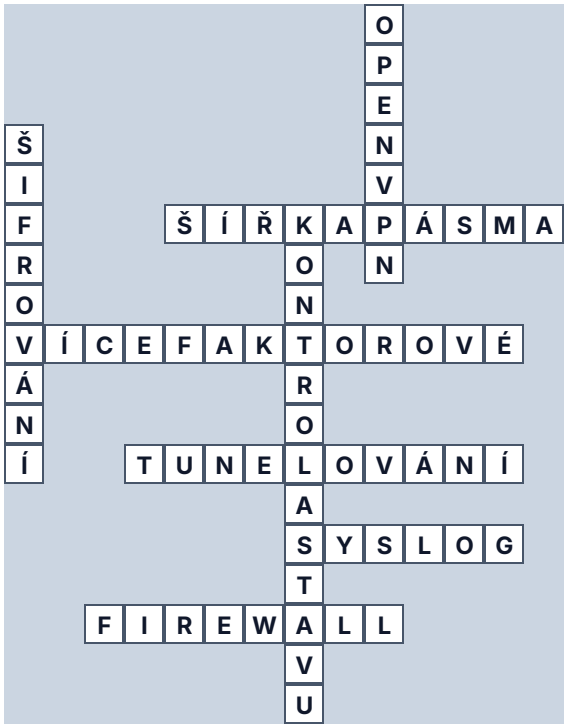
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

U	X	T	G	A	Ť	Y	A	Q	Ú	O	O	Z	P	H
V	R	Ť	H	Q	M	Ů	U	P	Ú	U	K	A	E	F
A	P	Ň	L	Á	O	S	Ů	Ě	F	R	Ř	X	I	Ý
T	J	J	Ů	J	Z	W	Á	Y	G	Q	J	R	I	Ž
S	I	Í	Ň	A	E	H	Á	P	T	O	E	A	J	É
A	W	E	K	Ž	K	Ď	L	Ř	A	W	L	Ň	J	A
L	Ě	P	K	O	Č	Ň	C	D	A	K	G	S	I	B
O	Á	P	S	M	Q	V	U	L	I	Ý	Ř	Ě	Y	Z
R	Š	F	Y	W	H	É	L	S	U	Ó	Ú	Í	K	S
T	S	D	Í	N	Á	V	O	R	F	I	Š	Ť	Š	T
N	V	Í	C	E	F	A	K	T	O	R	O	V	É	M
O	Q	L	O	P	E	N	V	P	N	Ň	T	H	K	Q
K	H	T	U	N	E	L	O	V	Á	N	Í	Z	P	M
W	Ú	O	Ý	Ř	Ř	Á	Á	M	Q	Ň	Á	L	I	É
Í	O	Ý	B	Ž	Ž	Z	B	Ň	Ů	Y	N	Č	É	P

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

3 vodorovně: ŠÍŘKAPÁSMA Limit datové kapacity sítě (10 písmen)

5 vodorovně: VÍCEFAKTOROVÉ Zabezpečení přihlášení vyžadující další tokeny (13 písmen)

6 vodorovně: TUNELOVÁNÍ Zapouzdření dat do zabezpečené cesty (10 písmen)

7 vodorovně: SYSLOG Centrální kolektor bezpečnostních logů (6 písmen)

8 vodorovně: FIREWALL Pravidla systému filtrování provozu (8 písmen)

SVISLÉ NÁPOVĚDY

1 svisle: OPENVPN Standardní protokol client-to-site (7 písmen)

2 svisle: ŠIFROVÁNÍ Kryptografické zakódování paketů (9 písmen)

4 svisle: KONTROLASTAVU Ověřování zdravotního stavu vzdáleného zařízení (13 písmen)

Klíč řešení přesmyček a šifry

Klíč k hodnocení aktivity s přesmyčkami slovní zásoby a výzvy Tajná šifra.

KLÍČ K PŘESMYČKÁM

1. KCOVAÍTRVOÉFE — **VÍCEFAKTOROVÉ**
2. VROONKALUSTAT — **KONTROLASTAVU**
3. ŠPMÁÍAAKSŘ — **ŠÍŘKAPÁSMA**
4. ONLÍEÁVTUN — **TUNELOVÁNÍ**
5. VNNEOPP — **OPENVPN**
6. OLSSGY — **SYSLOG**
7. VŠNÍÁRIOF — **ŠIFROVÁNÍ**
8. EIWLFLAR — **FIREWALL**

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"VZDÁLENÝ PŘÍSTUP VPN CHRÁNÍ FIREMNÍ ZAŘÍZENÍ"

Klíč k případovým studiím

A Případová studie 1: Vynucení MFA

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Obchodní analytik se při práci na dálku zkouší přihlásit do firemní databáze. Zadá správné uživatelské jméno i heslo, ale VPN portál přístup zablokuje a vyžaduje kód z fyzického tokenu.
- Doporučená strategie a řešení: Firemní VPN portál vynucuje přísnou politiku vícefaktorového ověřování (MFA) pro zabezpečení vzdálených přihlášení.

B Případová studie 2: Soulad s požadavky na stav zařízení

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Externí pracovník připojí svůj osobní notebook ke vzdálené firemní síti. VPN klient připojení okamžitě odpojí s upozorněním, že antivirové definice jsou zastaralé.
- Doporučená strategie a řešení: Brána vzdáleného přístupu provedla kontrolu stavu koncového zařízení a zablokovala je kvůli zastaralým bezpečnostním konfiguracím.